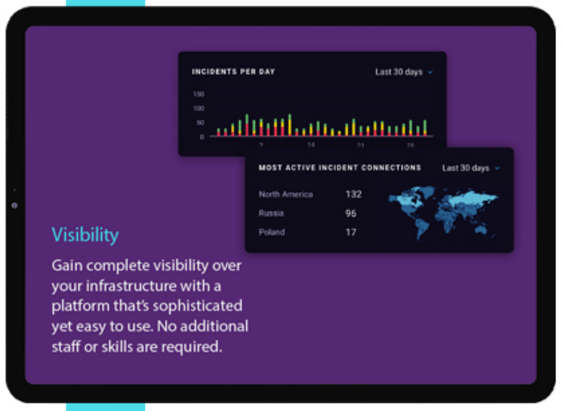
Endpoint Detection & Response

AI-Powered EDR Platform enables to Increase ROI and Manage & Secure More Endpoints



Portal Management Advantages

- NanoOS is resilient and invisible to attackers.
- Early detection of new and unknown threats, including ransomware.
- Minimum impact to endpoint performance.
- Highly customizable solution.
- Remote remediation of threats.
- Open APIs for easy integration with existing security stack .

Easy To Operate

- Intuitive management design.
- Benefits from management portal unprecedented levels of automation.
- Contain any situation in seconds with complete remediation guidance.
- Experience Threat Hunting made easy.
- Cyber assistant learns from analyst actions.
- Easily connect management to other components using a flexible API.
- Click-through response automations that provide analysts with a single, easy-to-use workflow.
- One-click detection strategies can be efficiently deployed across the whole customer base.

Created To Complement Your Operations

- Ease of Use
- Automated Reports
- Cloud Scanning
- Customizable Detection Strategies

- Increase Productivity
- Improve Efficiency
- Visibility
- Tracking

LOOPCLOUD

Endpoint Detection & Response

Complete Visibility from Endpoint to Infrastructure

Management portal monitors endpoints from outside the OS using the world's first NanoOS. The platform offers full visibility over the infrastructure, allowing real-time queries to endpoints.

Protection Beyond Legacy Solutions & Automated Threat Alerts

Management continuous learning A.I allows for detection of new techniques and previously unknown threats, that would escape detection from legacy and signature-based solutions. An early-warning system automatically identifies emerging threats, allowing security teams to perform a full security assessment before a breach happens.

Advanced Threat Detection with a Dual A.I. Engine

Management dual A.I engines work in concert to provide multiple points of detection. The first engine runs at the endpoint level, looking for malicious activity targeting a specific device. The second engine runs at the infrastructural level, looking for suspicious activity across the infrastructure.

Mitre ATT&CK™ Integration & Real-Time Hunting

Management offers real-time search of the infrastructure for presence of specific Indicators of Compromise (IOC), binaries and behaviors. The platform comes with a complete mapping of MITRETM Tactics & Techniques, as well as 120+ searchable parameters.

Compliance Ready

Management helps auditors identify gaps in compliance by scanning and analyzing endpoints. With real-time information on non-compliant endpoints, auditors can quickly remediate compliance issues as soon as they come up.

Rapid Incident Response and Ease-of-Use

Management interface enables analysts to respond to threats in under a minute. The UI directs analysts to the highest priority events, while the A.I. automatically reconstructs the incident, assessing its scope and impact on the infrastructure. The analysis workflow is simple and does not require additional security resources.

LOOPCLOUD